(19) 日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11) 特許出願公開番号

特開平11－312364

(43) 公開日　平成11年(1999) 11月９日

(51) Int. Cl.[6]	識別記号	ＦＩ		
G11B 20/10		G11B 20/10		H
H04N 5/765		H04N 5/781	510	L
5/781		5/92		H
5/92		7/13		Z
7/24				

審査請求　未請求　請求項の数12　ＯＬ　（全11頁）

(21) 出願番号　特願平10－118924

(22) 出願日　平成10年(1998) ４月28日

(71) 出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72) 発明者　勢木　真一
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

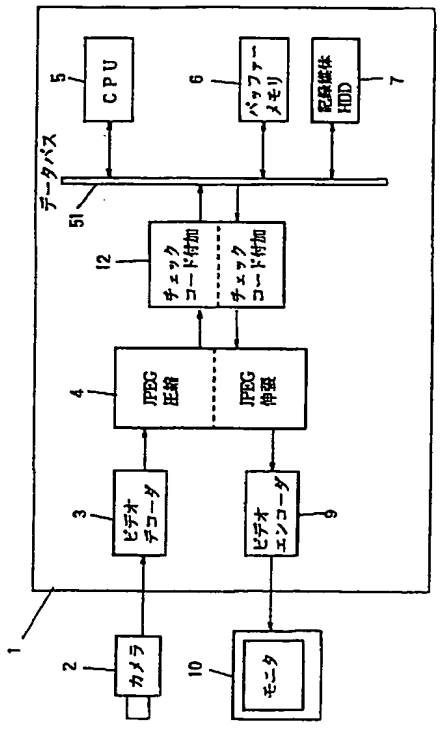
(74) 代理人　弁理士　前田　実

(54) 【発明の名称】ディジタルデータ記録装置、ディジタルデータ再生装置、及びチェックコード生成方法

(57) 【要約】

【課題】　媒体に記録されているディジタルデータが改変されたものかどうかを容易に検出できるディジタルデータ記録／再生装置を提供する。

【解決手段】　カメラ２から入力された映像はビデオデコーダ３によりディジタル映像データに変換され、ＪＰＥＧ圧縮伸張手段４でＪＰＥＧデータに圧縮される。このＪＰＥＧデータから、チェックコード付加解析器１２によってＪＰＥＧデータからサンプリングし、１０点のサンプリングデータを得さらに、このサンプリングデータに演算を加え、チェックコードを生成しＪＰＥＧデータのヘッダー内に付加する。このようにして生成したチェックコード付のＪＰＥＧデータを記録媒体７に記録する。その後に、何者かが、記録された映像データの改変しても再生時に高い精度で改変の有無を検出できる。



1

【特許請求の範囲】

【請求項１】　ディジタルデータを記録媒体に記録するディジタルデータ記録装置において、
ディジタルデータを圧縮するデータ圧縮手段と、
圧縮されたディジタルデータから一部のデータを第１の暗号関数に基づいて抽出する抽出手段と、
抽出されたデータを変数として第２の暗号関数に基づいてチェックコードを生成する生成手段と、
前記チェックコードを前記圧縮されたディジタルデータの所定位置に付加する付加手段とを備えたことを特徴とするディジタルデータ記録装置。

【請求項２】　前記第２の暗号関数は、サンプリング番号を変数とした暗証番号を変数とすることを特徴とする請求項１に記載のディジタルデータ記録装置。

【請求項３】　前記ディジタルデータがディジタル画像データであって、
このディジタル画像データを圧縮するＪＰＥＧ圧縮手段を備え、
前記チェックコードをＪＰＥＧ圧縮データのヘッダー内に付加したことを特徴とする請求項１または請求項２に記載のディジタルデータ記録装置。

【請求項４】　記録媒体に圧縮して記録されたディジタルデータを再生するディジタルデータ再生装置において、
圧縮ディジタルデータから一部のデータを第１の暗号関数に基づいて抽出する第１の抽出手段と、
前記第１の抽出手段で抽出されたデータを変数として第２の暗号関数に基づいて第１のチェックコードを生成する生成手段と、
圧縮ディジタルデータに付加されている第２のチェックコードを抽出する第２の抽出手段と、
前記第１のチェックコードと前記第２のチェックコードとを比較する比較手段と、
前記圧縮ディジタルデータを伸張する伸張手段とを備えたことを特徴とするディジタルデータ再生装置。

【請求項５】　記録媒体に圧縮して記録されたディジタルデータを再生するディジタルデータ再生装置において、
圧縮ディジタルデータから一部のデータを第１の暗号関数に基づいて抽出する第１の抽出手段と、
圧縮ディジタルデータに付加されているチェックコードを抽出する第２の抽出手段と、
前記第１の抽出手段で抽出されたデータと前記チェックコードとを第３の暗号関数に基づいて演算する演算手段と、
前記圧縮ディジタルデータを伸張する伸張手段とを備えたことを特徴とするディジタルデータ再生装置。

【請求項６】　前記ディジタルデータがディジタル画像データであって、
圧縮されたディジタル画像データを伸張するＪＰＥＧ伸張手段を備え、
前記チェックコードをＪＰＥＧ圧縮データのヘッダーから抽出したことを特徴とする請求項４または請求項５に記載のディジタルデータ再生装置。

2

【請求項７】　請求項１乃至請求項３のいずれかのディジタルデータ記録装置、或いは請求項４乃至請求項６のいずれかのディジタルデータ再生装置に使用されるチェックコードの生成方法であって、
圧縮されたディジタルデータの中から複数のサンプリングデータを抽出し、
前記抽出されたサンプリングデータとそのサンプリング番号を変数とした暗証番号とを変数としてチェックコードを生成することを特徴とするチェックコード生成方法。

【請求項８】　前記サンプリング番号を変数とした暗証番号は、暗号関数に基づいて生成されていることを特徴とする請求項７に記載のチェックコード生成方法。

【請求項９】　前記チェックコードは、抽出されたサンプリングデータと前記暗証番号とを変数とする算術加算関数によって生成されていることを特徴とする請求項７に記載のチェックコード生成方法。

【請求項１０】　前記チェックコードは、抽出されたサンプリングデータと前記暗証番号とを変数とするガロア体上での加算によって生成されていることを特徴とする請求項７に記載のチェックコード生成方法。

【請求項１１】　前記チェックコードは、抽出されたサンプリングデータと前記暗証番号とを変数とする排他的論理和演算によって生成されていることを特徴とする請求項７に記載のチェックコード生成方法。

【請求項１２】　前記サンプリングデータは、圧縮されたディジタルデータの中から暗号関数に基づいて抽出されていることを特徴とする請求項７乃至請求項１１のいずれかに記載のチェックコード生成方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、圧縮されたディジタルデータを記録媒体に記録し、或いは記録媒体から再生するディジタルデータ記録／再生装置、及びディジタルデータ記録／再生装置のディジタル画像の改変を検出するためのチェックコードの生成方法に関する。

【０００２】

【従来の技術】図８は、従来のディジタル画像記録再生装置の構成を示すブロック図である。１はディジタル画像記録再生装置、２はディジタル画像記録再生装置１に接続されたビデオカメラ、３はビデオカメラ２からのアナログ映像信号をディジタル映像データに変換するビデオデコーダ、４はＪＰＥＧ圧縮伸張手段、５はこのディジタル画像記録再生装置１の制御を行うＣＰＵ、５１はＣＰＵ５のデータバス、６はデータバス５１に接続されＪＰＥＧ圧縮伸張手段４で圧縮されたＪＰＥＧデータの

一時的格納などに用いるバッファーメモリ、７はＪＰＥＧデータを保存するためのＨＤＤ等の記録メディア、９は４：２：２プロファイルのディジタル映像データ（Ｙ、ＣＲ、ＣＢのデータ量が４：２：２のディジタル映像データ）をＮＴＳＣアナログ信号に変換するビデオエンコーダ、１１はディジタル画像記録再生装置１に接続されたモニタテレビである。

【０００３】つぎに、このディジタル画像記録再生装置で圧縮されたディジタルデータを記録媒体に記録し、或いは記録媒体から再生する動作について説明する。

【０００４】図９は、記録時の信号処理の流れを示すフローチャートである。処理ステップＳＴ２０において、ビデオカメラ２で撮影されたアナログ映像信号はディジタル画像記録再生装置１に入力され、ビデオデコーダ３によって４：２：２のディジタル映像データに変換される。次の処理ステップＳＴ２１では、ＪＰＥＧ圧縮伸張手段４によってＪＰＥＧデータに圧縮される。処理ステップＳＴ２２においては、ＪＰＥＧデータはデータバス５１を通って一旦バッファーメモリ６に格納され、バッファーメモリ６の中でタイムデートコード等を含んだヘッダーがＪＰＥＧデータに付加される。さらに処理ステップＳＴ２３において、ヘッダーが付加されたＪＰＥＧデータはデータバス５１を通って記録メディア７に記録される。

【０００５】図１０は、再生時の信号処理の流れを示すフローチャートであって、処理ステップＳＴ３０において、記録メディア７に記録されたＪＰＥＧデータはＣＰＵ５の制御によって一旦バッファーメモリ６に格納される。次に、処理ステップＳＴ３１ではヘッダー情報を抽出し、これによって時刻表示のデータなどを生成する。処理ステップＳＴ３２において、ＪＰＥＧデータはデータバス５１を通ってＪＰＥＧ圧縮伸張手段４に送られ、４：２：２ディジタル映像データに伸張される。最後に処理ステップＳＴ３３において、伸張された４：２：２ディジタル映像データをビデオエンコーダ９によってＮＴＳＣアナログ信号に変換し、モニタテレビ１０により再生映像を表示する。

【０００６】

【発明が解決しようとする課題】上記ディジタル画像記録再生装置１は、間欠記録の可能なディジタルタイムラプスレコーダとして鉄道、空港などの交通機関や、銀行など金融機関で、或いは化学実験や動植物の観察等の学術研究用途に広く用いられている。そこでは、記録された映像データを解析するため、記録の際にＪＰＥＧ圧縮されたデータを外部に出力するＳＣＳＩインターフェースやＲＳ２３２Ｃ端子を備えた装置が使用され、圧縮データをパソコンなどに送り、このパソコン等でＪＰＥＧ伸張することで通常の画像データに変換することができる。したがって記録された映像データは、コンピュータの画像処理ソフト等を用いて、コントラストの調整や輪郭強調や部分拡大などの修正を行うことができ、その後に再びＪＰＥＧ圧縮して保存することも可能である。

【０００７】しかし、修正された映像データを同じディジタル画像記録再生装置１に記録した場合、どれが元の記録データで、どれが修正後のデータなのか分からなくなってしまう恐れがあった。

【０００８】また、悪意を持った第三者が同様の方法で元の記録データを加工し、あるいは他のデータと入れ替えることが可能であるため、そのような画像データの一部が改変されたことを容易には検出することができなかった。これは、上記ディジタル画像記録再生装置１により記録された、犯罪などの証拠となり得る映像データを何者かが改変したり、あるいは犯罪の証拠となる映像データに対して部分的な追加や削除等が行われても、そのデータ自体からはデータの改変は検出できないことを意味する。このためディジタル映像データの証拠能力については、犯罪などを立証するに足りるものとは看做されていなかった。

【０００９】さらに、オリジナルデータであるか否かを確認するには、暗号技術を応用した方法がある。ところが、このような方法を動画像データに適用しようとすると、膨大で複雑な計算が必要となりコストの高いものになる問題がある。単純な確認方法としては、誤りの存在を検査するために使用されるチェックサム（Checksum）をチェックデータとして映像データに付加することも考えられる。しかし、加算によって付加されたチェックデータは容易に解読されてしまううえ、動画像データの場合にはチェックサムを付加するだけでもデータ処理量が多くなるため、専用のハードウェアを設ける必要があるという問題もあった。

【００１０】この発明は上記のような問題を解決するためのものであり、媒体に記録されているディジタルデータが改変されたものかどうかを容易に検出できるディジタルデータ記録／再生装置を提供することを目的としている。

【００１１】また、記録媒体に記録されている画像データが改変されたものであるかどうかを容易に検出でき、しかも解読のされにくいチェックコード生成方法を提供するものである。

【００１２】

【課題を解決するための手段】請求項１に係るディジタルデータ記録装置は、ディジタルデータを記録媒体に記録するディジタルデータ記録装置において、ディジタルデータを圧縮するデータ圧縮手段と、圧縮されたディジタルデータから一部のデータを第１の暗号関数に基づいて抽出する抽出手段と、抽出されたデータを変数として第２の暗号関数に基づいてチェックコードを生成する生成手段と、チェックコードを圧縮されたディジタルデータの所定位置に付加する付加手段とを備えたものである。

5

【００１３】請求項２に係るディジタルデータ記録装置では、第２の暗号関数は、サンプリング番号を変数とした暗証番号を変数とするものである。

【００１４】請求項３に係るディジタルデータ記録装置は、ディジタルデータがディジタル画像データであって、このディジタル画像データを圧縮するＪＰＥＧ圧縮手段を備え、チェックコードをＪＰＥＧ圧縮データのヘッダー内に付加したものである。

【００１５】請求項４に係るディジタルデータ再生装置は、記録媒体に圧縮して記録されたディジタルデータを再生するディジタルデータ再生装置において、圧縮ディジタルデータから一部のデータを第１の暗号関数に基づいて抽出する第１の抽出手段と、第１の抽出手段で抽出されたデータを変数として第２の暗号関数に基づいて第１のチェックコードを生成する生成手段と、圧縮ディジタルデータに付加されている第２のチェックコードを抽出する第２の抽出手段と、第１のチェックコードと第２のチェックコードとを比較する比較手段と、圧縮ディジタルデータを伸張する伸張手段とを備えたものである。

【００１６】請求項５に係るディジタルデータ再生装置は、記録媒体に圧縮して記録されたディジタルデータを再生するディジタルデータ再生装置において、圧縮ディジタルデータから一部のデータを第１の暗号関数に基づいて抽出する第１の抽出手段と、圧縮ディジタルデータに付加されているチェックコードを抽出する第２の抽出手段と、第１の抽出手段で抽出されたデータとチェックコードとを第３の暗号関数に基づいて演算する演算手段と、圧縮ディジタルデータを伸張する伸張手段とを備えたものである。

【００１７】請求項６に係るディジタルデータ再生装置は、ディジタルデータがディジタル画像データであって、圧縮されたディジタル画像データを伸張するＪＰＥＧ伸張手段を備え、チェックコードをＪＰＥＧ圧縮データのヘッダーから抽出したものである。

【００１８】請求項７に係るチェックコード生成方法は、ディジタルデータ記録装置、或いはディジタルデータ再生装置に使用されるチェックコードの生成方法であって、圧縮されたディジタルデータの中から複数のサンプリングデータを抽出し、抽出されたサンプリングデータとそのサンプリング番号を変数とした暗証番号とを変数としてチェックコードを生成するものである。

【００１９】請求項８に係るチェックコード生成方法では、サンプリング番号を変数とした暗証番号は、暗号関数に基づいて生成されている。

【００２０】請求項９に係るチェックコード生成方法では、チェックコードは、抽出されたサンプリングデータと暗証番号とを変数とする算術加算関数によって生成されている。

【００２１】請求項１０に係るチェックコード生成方法では、チェックコードは、抽出されたサンプリングデータと暗証番号とを変数とするガロア体上での加算によって生成されている。

6

【００２２】請求項１１に係るチェックコード生成方法では、チェックコードは、抽出されたサンプリングデータと暗証番号とを変数とする排他的論理和演算によって生成されている。

【００２３】請求項１２に係るチェックコード生成方法では、サンプリングデータは、圧縮されたディジタルデータの中から暗号関数に基づいて抽出されている。

【００２４】

【発明の実施の形態】実施の形態１．図１は、この発明の実施の形態１におけるディジタル画像記録再生装置の構成を示すブロック図である。従来例の対応する図面（図８）と対応する部分には同一の符号を付けている。

【００２５】図において、１はディジタル画像記録再生装置、２はディジタル画像記録再生装置１に接続されたビデオカメラ、３はビデオカメラ２からのアナログ映像信号を４：２：２プロファイルのディジタル映像データに変換するビデオデコーダ、４はＪＰＥＧ圧縮伸張手段、１２はＪＰＥＧ圧縮データに対して固有のチェックコードを付加し、解析するチェックコード付加解析器、５はこのディジタル画像記録再生装置１の制御を行うＣＰＵ、５１はＣＰＵ５のデータバス、６はデータバス５１に接続されＪＰＥＧ圧縮伸張手段４で圧縮されたＪＰＥＧデータの一時的格納などに用いるバッファーメモリ、７はＪＰＥＧデータを保存するためのＨＤＤ等の記録メディア、９は４：２：２プロファイルのディジタル映像データをＮＴＳＣアナログ信号に変換するビデオエンコーダ、１０はディジタル画像記録再生装置１に接続されたモニタテレビである。

【００２６】図２は、記録時の信号処理の流れを示すフローチャートであって、処理ステップＳＴ２０～２３は図９の各処理に対応するものである。処理ステップＳＴ２０においてビデオカメラ２で撮影されたアナログ映像信号はディジタル画像記録再生装置１に入力されビデオデコーダ３によって４：２：２のディジタル映像データに変換される。次に、処理ステップＳＴ２１ではＪＰＥＧ圧縮伸張手段４によってＪＰＥＧデータに圧縮される。処理ステップＳＴ４０においてサンプリングされたＪＰＥＧデータは、処理ステップＳＴ４１においてチェックコード付加解析器１２による演算で所定のチェックコードが生成される。このチェックコードは、処理ステップＳＴ２１で圧縮されたＪＰＥＧデータと共にデータバス５１を通って一旦バッファーメモリ６に格納される。

【００２７】次に、処理ステップＳＴ４１におけるチェックコードの生成方法について述べる。まず、処理ステップＳＴ４０においてＪＰＥＧデータＤ（ｉ）の中から、各１バイトのサンプリングデータとして、例えば１０点（ｎ＝０～９）を選んで各１バイトのサンプリング

データＳ（ｎ）を第１の暗号関数、例えば以下の式（１）に基づいて抽出する。

$$S(n)=D(a\times n+b) \quad \cdots(1)$$

ただし、ｎはサンプリング番号、ａ，ｂは定数である。

【００２９】処理ステップＳＴ４１では、これらのサンプリングデータＳ（０）～Ｓ（９）を変数として、次式（２）に示される暗号関数（Ｆ（＊）：第２の暗号関数）に基づいて演算を施し、チェックコードＣ（ｎ）を生成する。

$$C(n)=F(S(n),X(n)) \quad \cdots(2)$$

なお、Ｘ（ｎ）は暗証番号配列を決定するための暗号関数である。

【００３０】

【００３１】このＦ（＊）の演算はチェックコードのルールを他者に解析されにくくするためのもので、この秘密とされる暗号関数Ｆ（＊）だけでなく、暗証番号配列を決定する暗号関数Ｘ（ｎ）、及び上記定数ａ，ｂをも秘密にしておけば、チェックコードＣ（ｎ）の解析は非常に困難になる。

【００３２】図４は、チェックコードの生成方法を模式的に示した図である。図において、６１０は圧縮されたＪＰＥＧデータ、６２０はその先頭のタイムデートコード等を含んだヘッダーデータ、６２１はヘッダー内に付加されたチェックコードである。

【００３３】生成されるチェックコードの具体例としては、秘密の関数Ｆ（＊）を算術加算、暗証番号配列を決定するＸ（ｎ）＝ｎとしたとき、式（２）のチェックコードＣ（ｎ）を書き換えると、次の式（３）になり、チェックコードの配列は図５のようになる。

【００３４】

$$C(n)=S(n)+n \quad \cdots(3)$$

ただし、ｎはサンプリング番号で０～９である。

【００３５】処理ステップＳＴ４２によってこのチェックコード６２１とタイムデートコード等を含んだヘッダーデータ６２０を生成し、処理ステップＳＴ２２で上記ＪＰＥＧデータ６１０に付加する。なお、このヘッダーデータ６２０はＪＰＥＧ規格に準拠した形で構成される。処理ステップＳＴ２３において、このヘッダーデータ６２０が付加されたＪＰＥＧデータ６１０はデータバス５１を通って記録メディア７に記録される。

【００３６】次に、再生時の動作について説明する。図３は、再生時の信号処理の流れを示すフローチャートであって、処理ステップＳＴ３０～３３は図１０の各処理に対応するものである。

【００３７】処理ステップＳＴ３０において記録メディア７に記録されているＪＰＥＧデータは、ＣＰＵ５の制御によって一旦バッファーメモリ６に格納される。このバッファーメモリ６に格納されたＪＰＥＧデータから処理ステップＳＴ３１でヘッダー情報が抽出され、さらに処理ステップＳＴ４３によってヘッダーからチェックコードが抽出される。

【００３８】また、処理ステップＳＴ３１、４３に並行して、処理ステップＳＴ４０においてバッファーメモリ６に格納されたＪＰＥＧデータから記録時と同様の方法でチェックコードが生成される。すなわち、上記式（１）によってＪＰＥＧデータＤ（ｉ）の中から記録時と同じ１０点（ｎ＝０～９）のサンプリングデータＳ（ｎ）を求める。処理ステップＳＴ４１では、１０点のサンプリングデータＳ（ｎ）に上記式（３）に示される演算を施して、チェックコードＣ（ｎ）を生成する。この処理ステップＳＴ４１での演算は、記録時に行われたチェックコードを求めるための演算と同一の処理であって、通常は処理ステップＳＴ４３で抽出したチェックコードと同一のものとなるが、記録後にデータの改変が行われているときは異なるチェックコードとして求められる。

【００３９】その後、処理ステップＳＴ４５において、処理ステップＳＴ４３で抽出したチェックコードと処理ステップＳＴ４１によって算出したチェックコードを比較する。もし、２つのチェックコードが互いに異なっていた場合には、記録後にデータの改変が行われたものであるから、処理ステップＳＴ４６によってモニタテレビ１０に対して警告表示を出すように指令する。これにより、再生された映像データが一旦記録メディア７に格納された後に何者かによって改変を加えられた旨の警告がなされる。

【００４０】処理ステップＳＴ３２では、ＪＰＥＧデータがデータバス５１を通ってＪＰＥＧ圧縮伸張手段４に送られ、再びディジタル映像データに伸張される。この伸張されたディジタル映像データは、処理ステップＳＴ３３において、ビデオエンコーダ９によってＮＴＳＣアナログ信号に変換され、モニタテレビ１０に再生映像を表示する。処理ステップＳＴ４６で指令された警告は、この時の再生映像の上に重ねて表示し、改ざんされたデータであることを明示する。こうして再生中の映像データが、何者かによって改ざんされたものであることを明らかにできる。

【００４１】以上のように、圧縮されたＪＰＥＧデータの一部をサンプリングしてチェックコードを生成し、ディジタル映像データとともに記録メディア７に格納するようにしたので、非常に少ないデータの処理量で記録されているディジタルデータが改変されたものかどうかを容易に検出することができる。

【００４２】つぎに、何者かが記録された映像データを、一旦、ＪＰＥＧ伸張することで通常の画像データに変換して、その後にコンピュータの画像処理ソフト等を用いて画像データの一部を改変した後、再びＪＰＥＧ圧縮して元の記録データと入れ替えてしまうような場合について考察する。映像データを改変した範囲が映像データの一部の限られた領域だけであっても、ＪＰＥＧ圧縮処理の過程で行われるＤＣＴ符号化、あるいはハフマン符号化によって圧縮された後のＪＰＥＧデータでは、一部改変による元の映像データの影響が圧縮後のＪＰＥＧデータの全域に広がってしまう。このため、１０点程度の少ないサンプリングポイントを使用するだけであっても、映像データの改変を確実に検出することができる。

【００４３】また、改変した映像データに対して新たにチェックコードを付けて、改変したことを分からなくすることも不可能に近い。何故ならば、式（１）および式（２）で示された映像データからのサンプリングルールやチェックコードの演算方法は暗号関数に基づくものであり、暗証番号配列を決定するための暗号関数を含めて全ての暗号関数が知られていない限りでは、第三者がチェックコード自体を解析することは極めて困難だからである。したがって、この実施の形態１のディジタル画像記録再生装置は、映像データの証拠能力を高めるうえでも有効である。

【００４４】以上述べたように、実施の形態１のディジタルデータ記録再生装置におけるディジタル画像の改変を検出するためのチェックコードの生成方法は、簡便な方法でありながら、非常に高い検出能力と、悪意を持った第三者による解析に対しても高い信頼性を持っている。このため犯罪などが発生した場合においても、本実施の形態のディジタルデータ記録装置で記録された映像データは高い証拠能力がある。

【００４５】なお、チェックコードはＪＰＥＧ圧縮したヘッダーデータの未使用の予約領域に格納することで、通常のチェックコードを付加、解析する機能のないディジタルデータ記録再生装置であっても再生することが可能である。

【００４６】実施の形態２．実施の形態１では、チェックコードＣを生成する際の暗号関数Ｆ（＊）として、式（２）に示すような通常の算術加算を用いたが、これは他の関数であっても良い。例えばガロア体（有限体）の加法演算などを用いて、チェックコードを生成することもできる。

【００４７】実施の形態１では、８ｂｉｔデータに対して通常の算術加算を行っているために加算結果に桁上がりが発生した場合に、演算結果が８ｂｉｔデータでは収まらなり、桁上がり部分の切り捨てが行われる。このため、異なるサンプリングデータに対して同一のチェックコードを生成することになるが、そうすると映像データの改変を見過ごしてしまう可能性がある。そこで、暗号関数Ｆ（＊）として式（２）のような通常の算術加算の代わりにガロア体上の加算を用いることで、サンプリングデータが異なれば必ず異なるチェックコードが生成される。これによって、映像データの改変を見過ごしてしまう可能性を小さくすることができる。

【００４８】実施の形態３．実施の形態１では、チェックコードＣ（ｎ）を生成する際に、式（２）に示すような暗号関数Ｆ（＊）として通常の算術加算を用いたが、これは他の関数であっても良く、例えば排他的論理和演算を用いてもよい。図６に示すように、ヘッダーデータ（上位）と暗証番号配列Ｘ（１０）、ヘッダーデータ（下位）と暗証番号配列Ｘ（１１）、サンプリングデータＳ（０）と暗証番号配列Ｘ（０）、等の間で排他的論理和演算を実行する。このような演算によれば、実施の形態２と同様に、サンプリングデータが異なれば必ず異なるチェックコードを生成することができる。

【００４９】この方法は、実施の形態２で用いたガロア体の加算を用いる方法よりも簡単にチェックコードを生成できる効果がある。

【００５０】また、図６に示すようにヘッダーデータとは別に暗号関数のバージョン情報をチェックコードに付加し、このバージョン情報に応じて映像データからのサンプリングルールやチェックコードの演算方法、及び暗証番号配列を決定するための暗号関数を変更することもできる。ここで、バージョン情報とはそれぞれ異なる暗号関数を記憶する複数のバージョン（Ver. 1. 0、Ver. 2. 0等）を特定する情報であって、装置毎に、あるいは記録期間毎に使用した暗号関数のバージョン情報がチェックコードに付加される。

【００５１】こうすれば、あるバージョンの暗号関数が悪意を持った第三者に知られた場合でも、それ以外のバージョンの暗号関数で生成されたチェックコードの信頼性を保つことができ、画像データの改変を防止できる効果がある。

【００５２】また、図４に示すヘッダー６２０を、例えば挿入されるチェックコード６２１よりも前の部分（上位部分）と後ろの部分（下位部分）とに分割し、上位部分のヘッダーを加算して上位のヘッダーデータとし、下位部分のヘッダーを加算して下位のヘッダーデータとする。これら上位、下位のヘッダーデータと暗証番号配列Ｘ（１０），Ｘ（１１）との排他的論理和演算をおこなって、サンプリングデータから生成されたチェックコードに付加する。このようなチェックコードを用いることで、ヘッダー情報自体が改変された場合にもそれを検出することができる。ヘッダー部分には、ＪＰＥＧデータの伸張に必要な情報の他、日時情報やカメラ番号などの重要な情報が記録されているため、このようなヘッダー部分の改変の検出手段を設けることで、さらに信頼性の高い装置を得ることができる。

【００５３】実施の形態４

実施の形態１～３では、秘密の関数Ｆ（＊）として式（２）に示すように、１つのサンプリングデータと１つの暗証番号を用いて、一つのチェックコードを算出したが、以下の式（４）に示すように、複数のサンプリング

Ｃ（ｎ）＝Ｆ（Ｓ（ｎ），Ｓ（ｎ＋１），Ｘ（ｎ），Ｘ（ｎ＋１））　…（４）

この場合には、悪意を持った第三者によるチェックコードの解析をより一層困難なものにし、チェックコードの信頼性を上げる効果がある。

【００５５】実施の形態５．実施の形態１では、式（１）に示す一次式で予め決められた定数ａ，ｂを用い

Ｓ（ｎ）＝Ｄ（（Ｎ＋２）ｎ／１６）　…（５）

となり、１６分割されたデータのうちの３番目のデータから１０点をサンプリングできる。こうすればサンプリングポイントの数は変わらないので、ＪＰＥＧデータが小さい場合でも改変検出の精度が低くならない効果がある。また、ＪＰＥＧデータのデータ量によってサンプリングポイントを容易に変更できるので、悪意を持った第三者によるチェックコードの解析をより一層困難なものにし、チェックコードの信頼性を上げる効果がある。

【００５７】実施の形態６．実施の形態１では、サンプリングデータＳ（ｎ）をサンプリングする方法として、式（１）に示す一次式を用いたが、他の方法でサンプリングしても良い。例えば、対数、三角関数などの他の関数は、その例である。また、乱数を用いてサンプリングする方法や、秘密の暗証番号を用いてサンプリング位置を変えても良い。この場合、悪意を持った第三者によるチェックコードの解析をより一層困難なものにし、チェックコードの信頼性を上げる効果がある。

【００５８】実施の形態７．図７は、この発明の実施の形態７における再生時の信号処理の流れを示すフローチャートであって、処理ステップＳＴ３０～３３は図１０

Ｖ（ｎ）＝Ｓ（ｎ）－Ｃ（ｎ）＋ｎ　…（６）

のような演算を設定しておけば、処理ステップＳＴ４８における演算結果Ｖ（ｎ）＝０であるかどうかによって、改変の有無が判断できる。

【００６２】したがって、処理ステップＳＴ４８においてＶ（ｎ）≠０であれば、処理ステップＳＴ４６によってモニタテレビ１０に対して警告表示を出すように指令して、何者かによって改変されたものであることを知らせることが可能になる。

【００６３】なお、上記実施の形態１～７では、いずれも画像データの圧縮方法としてＪＰＥＧ圧縮を用いているが、ＭＰＥＧ１、ＭＰＥＧ２、ＭＰＥＧ４、Ｈ．２６１など、他の圧縮方法による映像データに対しても同様に有効である。

【００６４】また、記録装置として間欠記録を行うディジタルタイムラプスレコーダ以外に通常の連続記録装置にも適用でき、同様の効果を奏する。

【００６５】また、上記実施の形態１～７では画像データの記録について説明したが、例えば音声データ等、他

データと複数の暗証番号を用いて、一つのチェックコードを算出してもよい。

【００５４】

ていたが、ＪＰＥＧデータのデータ量が変わってもサンプリングポイントの数ｎが変わらないように、定数ａ，ｂをデータ量に応じて変更するようにしてもよい。

【００５６】例えば、Ｎを全データ数、ａ＝Ｎ／１６，ｂ＝２ａのように決定しておけば、

の各処理に対応するものである。

【００５９】処理ステップＳＴ３０において記録メディア７に記録されているＪＰＥＧデータは、ＣＰＵ５の制御によって一旦バッファーメモリ６に格納される。このバッファーメモリ６に格納されたＪＰＥＧデータから処理ステップＳＴ３１でヘッダー情報が抽出され、さらに処理ステップＳＴ４３によってヘッダーからチェックコードが抽出される。

【００６０】また、処理ステップＳＴ３１、４３に並行して、処理ステップＳＴ４０では、このバッファーメモリ６に格納されたＪＰＥＧデータから式（１）によってサンプリングデータＳ（ｎ）を求める。処理ステップＳＴ４７では、このサンプリングデータＳ（ｎ）と処理ステップＳＴ４３によって抽出されたチェックコードとが直接に演算され、改変されたデータかどうかのチェックが行なわれる。

【００６１】処理ステップＳＴ４７における演算としては、例えば記録時のチェックコードが式（３）により生成されている場合には、

の種類のデータを記録再生するものであっても同様の効果を奏する。

【００６６】さらに、上記実施の形態１～７ではチェックコードの付加解析器１２に専用の回路を設けているが、これらの処理は非常に簡便に行うことができるので、ＣＰＵ５によってソフトウェア的に実行するようにしてハードウェアを簡素化することも可能である。

【００６７】

【発明の効果】この発明は、以上説明したように構成されているので、以下に示すような効果を奏する。

【００６８】請求項１に記載したディジタルデータ記録装置によれば、媒体に記録されているディジタルデータが改変されたものかどうかを容易に検出できる。

【００６９】請求項２の装置では、第２の暗号関数は、サンプリング番号を変数とした暗証番号を変数とするので、チェックコードの解析は非常に困難になり、映像データの証拠能力を高めるうえで有効である。

【００７０】請求項３の装置では、ディジタルデータが

ディジタル画像データである場合に、このディジタル画像データを圧縮するＪＰＥＧ圧縮手段を備え、チェックコードをＪＰＥＧ圧縮データのヘッダー内に付加したので、ディジタル画像の改変を簡便な方法で検出でき、悪意を持った第三者の改変を高い信頼性で防止できる。

【００７１】請求項４に記載したディジタルデータ再生装置によれば、再生されているディジタルデータが改変されたものかどうかを容易に検出できる。

【００７２】請求項５に記載したディジタルデータ再生装置によれば、簡単な演算だけで再生されているディジタルデータが改変されたものかどうかを容易に検出できる。

【００７３】請求項６の装置では、ディジタルデータがディジタル画像データである場合に、圧縮されたディジタル画像データを伸張するＪＰＥＧ伸張手段を備え、チェックコードをＪＰＥＧ圧縮データのヘッダーから抽出したので、ディジタル画像の改変を簡便な方法で検出でき、悪意を持った第三者の改変を高い信頼性で防止できる。

【００７４】請求項７に記載したチェックコードの生成方法によれば、記録媒体に記録されている画像データが改変されたものであるかどうかを容易に検出でき、しかも解読のされにくいチェックコードを生成できる。

【００７５】請求項８の方法では、サンプリング番号を変数とした暗証番号が、暗号関数に基づいて生成されているので、チェックコードの解析は非常に困難になり、映像データの証拠能力を高めるうえで有効である。

【００７６】請求項９の方法では、チェックコードが、抽出されたサンプリングデータと暗証番号とを変数とする算術加算関数によって生成されているので、少ないサンプリングポイントを使用するだけで、映像データの改変が確実に検出できる。

【００７７】請求項１０の方法では、チェックコードが、抽出されたサンプリングデータと暗証番号とを変数とするガロア体上での加算によって生成されているので、サンプリングデータが異なれば必ず異なるチェックコードが生成され、映像データの改変を見過ごしてしまう可能性を小さくすることができる。

【００７８】請求項１１の方法では、チェックコードが、抽出されたサンプリングデータと暗証番号とを変数とする排他的論理和演算によって生成されているので、簡単にチェックコードを生成できる。

【００７９】請求項１２の方法では、サンプリングデータが、圧縮されたディジタルデータの中から暗号関数に基づいて抽出されているので、解読のされにくいチェックコードを生成できる。

【図面の簡単な説明】

【図１】　この発明の実施の形態１に係るディジタル画像記録再生装置の構成を示すブロック図である。

【図２】　この発明の実施の形態１に係る記録動作を示すフローチャートである。

【図３】　この発明の実施の形態１に係る再生動作を示すフローチャートである。

【図４】　この発明の実施の形態１に係るチェックコードの生成を模式的に示す図である。

【図５】　この発明の実施の形態１に係るチェックコードを示す図である。

【図６】　この発明の実施の形態３に係るチェックコードを示す図である。

【図７】　この発明の実施の形態７に係る再生動作を示すフローチャートである。

【図８】　従来のディジタル画像記録再生装置の構成を示すブロック図である。

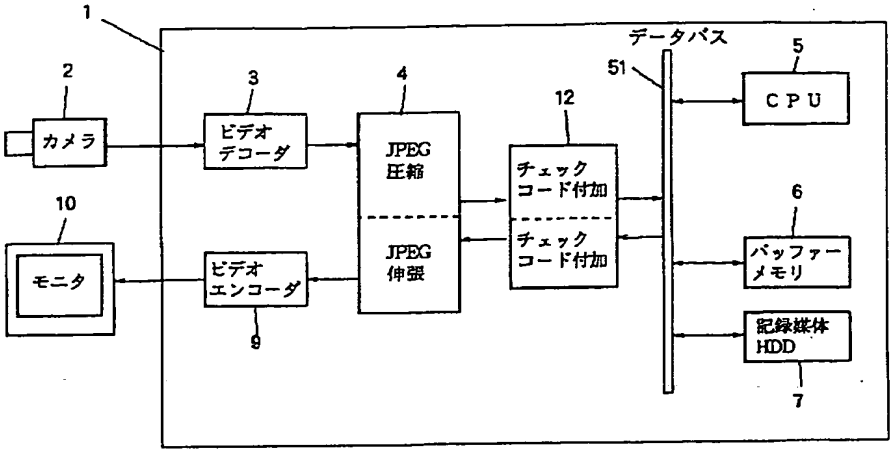
【図９】　従来のディジタル画像記録再生装置の記録動作を示すフローチャートである。

【図１０】　従来のディジタル画像記録再生装置の再生動作を示すフローチャートである。

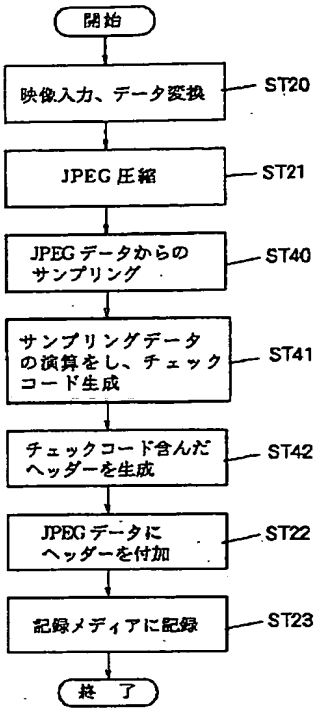
【符号の説明】

１　ディジタル画像記録再生装置、２　ビデオカメラ、３　ビデオデコーダ、４　ＪＰＥＧ圧縮伸張手段、５　ＣＰＵ、６　バッファーメモリ、７記録メディア、８　通信インターフエース、９　ビデオエンコーダ、１０モニタテレビ、１２　チェックコード付加解析器、５１　データバス。

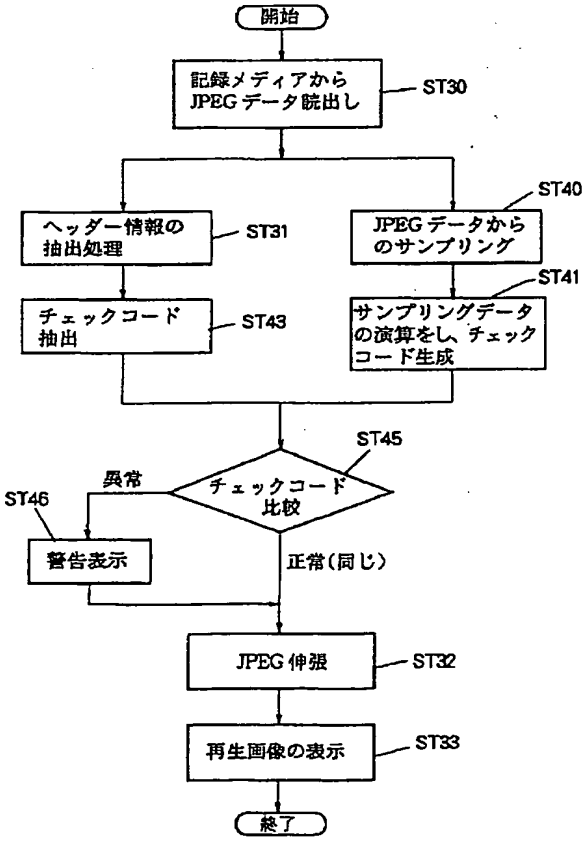
【図１】


1
2
カメラ
3
ビデオ
デコーダ
4
JPEG
圧縮
JPEG
伸張
12
チェック
コード付加
チェック
コード付加
データバス
51
5
ＣＰＵ
6
バッファー
メモリ
記録媒体
HDD
7
10
モニタ
ビデオ
エンコーダ
9

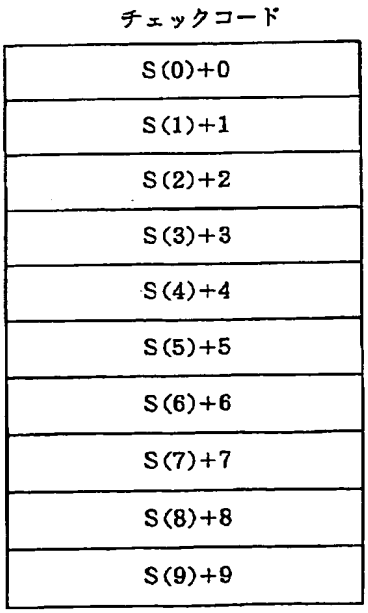
【図２】


開始
映像入力、データ変換
ST20
JPEG 圧縮
ST21
JPEG データからの
サンプリング
ST40
サンプリングデータ
の演算をし、チェック
コード生成
ST41
チェックコード含んだ
ヘッダーを生成
ST42
JPEG データに
ヘッダーを付加
ST22
記録メディアに記録
ST23
終 了

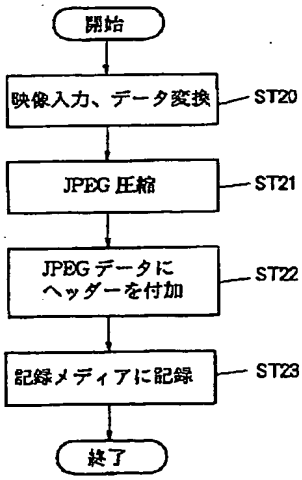
【図３】


開始
記録メディアから
JPEG データ読出し
ST30
ヘッダー情報の
抽出処理
ST31
JPEG データから
のサンプリング
ST40
チェックコード
抽出
ST43
サンプリングデータ
の演算をし、チェック
コード生成
ST41
チェックコード
比較
ST45
異常
ST46
警告表示
正常(同じ)
JPEG 伸張
ST32
再生画像の表示
ST33
終了

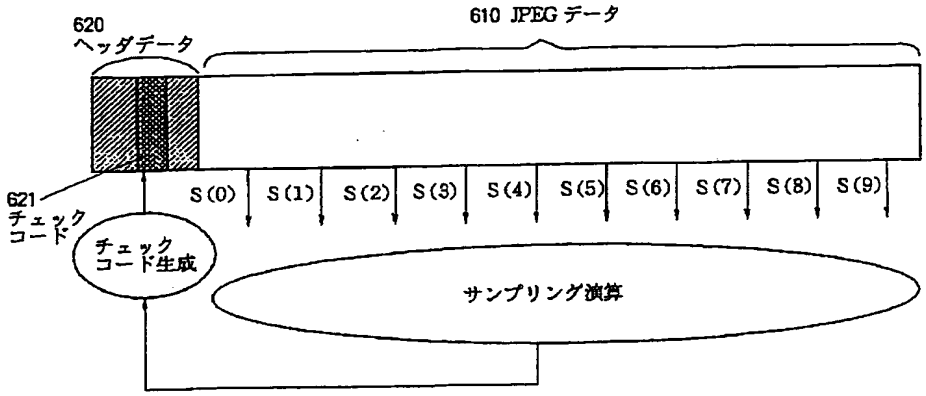
【図５】


チェックコード
S(0)+0
S(1)+1
S(2)+2
S(3)+3
S(4)+4
S(5)+5
S(6)+6
S(7)+7
S(8)+8
S(9)+9

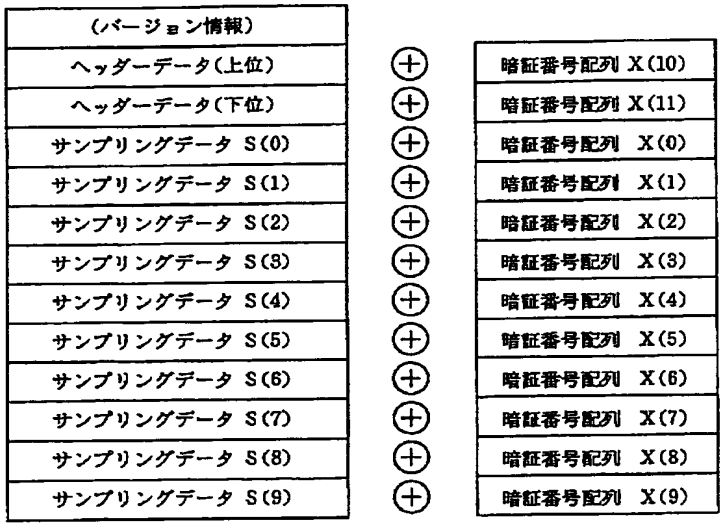
【図９】


開始
映像入力、データ変換
ST20
JPEG 圧縮
ST21
JPEG データに
ヘッダーを付加
ST22
記録メディアに記録
ST23
終了

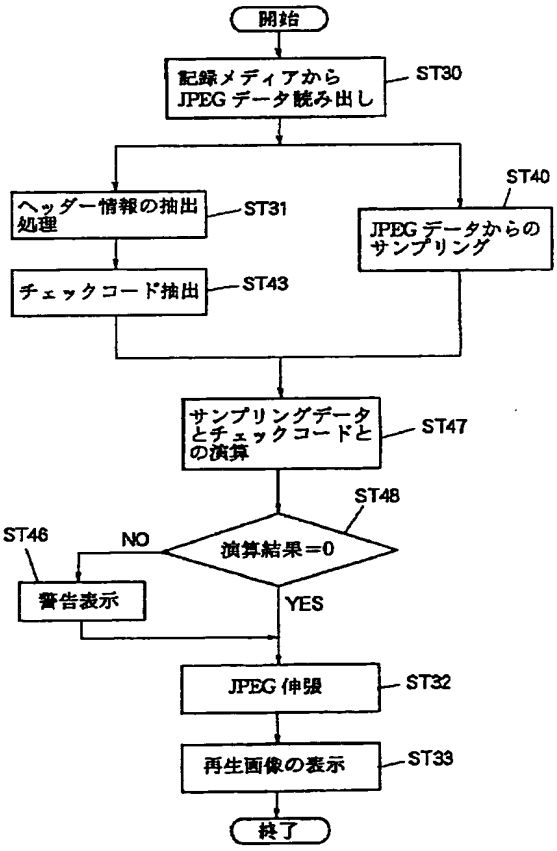
【図４】


620
ヘッダデータ
610 JPEG データ
621
チェック
コード
S(0)
S(1)
S(2)
S(3)
S(4)
S(5)
S(6)
S(7)
S(8)
S(9)
チェック
コード生成
サンプリング演算

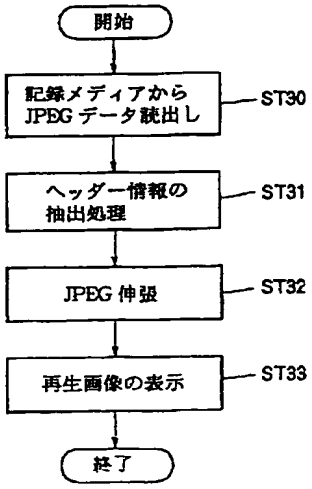
【図６】


(バージョン情報)
ヘッダーデータ(上位)
ヘッダーデータ(下位)
サンプリングデータ S(0)
サンプリングデータ S(1)
サンプリングデータ S(2)
サンプリングデータ S(3)
サンプリングデータ S(4)
サンプリングデータ S(5)
サンプリングデータ S(6)
サンプリングデータ S(7)
サンプリングデータ S(8)
サンプリングデータ S(9)
暗証番号配列 X(10)
暗証番号配列 X(11)
暗証番号配列 X(0)
暗証番号配列 X(1)
暗証番号配列 X(2)
暗証番号配列 X(3)
暗証番号配列 X(4)
暗証番号配列 X(5)
暗証番号配列 X(6)
暗証番号配列 X(7)
暗証番号配列 X(8)
暗証番号配列 X(9)

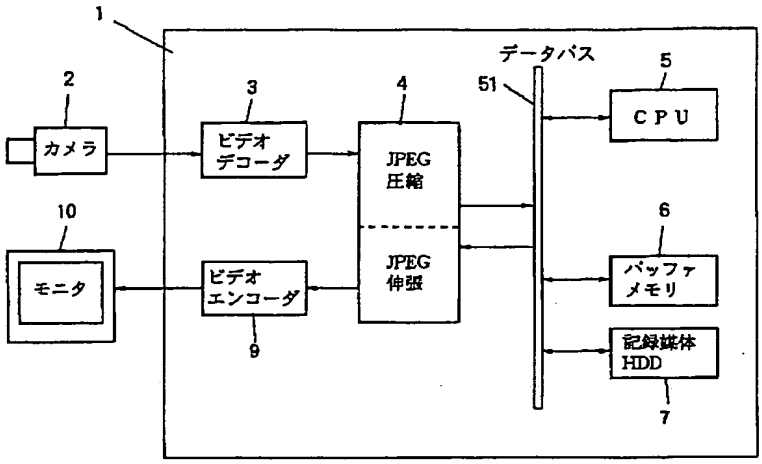
【図７】


開始
記録メディアから
JPEG データ読み出し
ST30
ヘッダー情報の抽出
処理
ST31
チェックコード抽出
ST43
ST40
JPEG データからの
サンプリング
サンプリングデータ
とチェックコードと
の演算
ST47
ST48
演算結果＝0
NO
YES
ST46
警告表示
JPEG 伸張
ST32
再生画像の表示
ST33
終了

【図１０】


開始
記録メディアから
JPEG データ読出し
ST30
ヘッダー情報の
抽出処理
ST31
JPEG 伸張
ST32
再生画像の表示
ST33
終了

【図８】


1
2
カメラ
3
ビデオ
デコーダ
4
JPEG
圧縮
JPEG
伸張
データバス
51
5
ＣＰＵ
6
バッファ
メモリ
記録媒体
HDD
7
10
モニタ
ビデオ
エンコーダ
9